Warren A. Stramiello
(warren@law.stramiello.net)
Stramiello Law Firm
5 Masefield Lane
Hartsdale, NY 10530
Tel: (678) 619-1337
Fax: (415) 423-3571

Ridder, Costa & Johnstone LLP
Chris K. Ridder (pro hac vice pending)
(chris@rcjlawgroup.com)
12 Geary Street, Suite 701
San Francisco, CA 94108
Tel: (415) 391-3311
Fax: (415) 358-4975
Attorneys for Non-Party Internet Security Research Group, dba Let's Encrypt

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

HERBALIST & ALCHEMIST, INC. Plaintiff, v. ALURENT PRODUCTS, INC. and WILL CLARENT, Defendants.	16-CIV-09204 (ER)

NON-PARTY LET'S ENCRYPT'S MEMORANDUM OF LAW IN RESPONSE TO ORDER TO SHOW CAUSE

Table of Contents

Table of Authorities

Non-party Internet Security Research Group, dba Let's Encrypt ("Let's Encrypt"), respectfully submits this memorandum of law in opposition to the application for contempt filed by Plaintiff Herbalist & Alchemist, Inc. ("Plaintiff"), and the accompanying Order to Show Cause entered on July 20, 2017.

PRELIMINARY STATEMENT

Plaintiff seeks to wield a default judgment, entered against absent defendants, to try to force more than a dozen non-parties to act as Plaintiff demands, under threat of contempt of court. Let's Encrypt, one of those non-parties, specially appears before the Court solely to contest jurisdiction, enforceability, and validity of the Default Judgment[1], and to oppose the Order to Show Cause[2], to the extent that they purport to direct Let's Encrypt to revoke certain DV Certificates.

Over eight months have passed since Plaintiff filed its complaint, alleging trademark infringement by two defendants. During this time, Plaintiff has never sought to amend its complaint or otherwise join Let's Encrypt as a party to this action, nor has it ever brought a separate action against Let's Encrypt. Plaintiff did not mention Let's Encrypt or SSL Certificates in its request for Default Judgment, nor were they mentioned in the as-issued Default Judgment or in Plaintiff's letter motion re-opening the case. When Plaintiff first approached Let's Encrypt in late May 2017, Let's Encrypt informed Plaintiff

---

[1] *March 8, 2017, Default Judgment Against Defendants Alurent Products, Inc., and Will Clarent (Docket #28) (the "Default Judgment").*

[2] *July 20, 2017, Order to Show Cause for Contempt for Violation of A Court Order and Permanent Injunction and To Enforce Compliance (Docket #34) (the "Order to Show Cause" or "OSC").*

that DV Certificates were not related to infringement and that revoking such certificates did not seem to be within the scope of the Default Judgment.[3] Let's Encrypt offered to discuss the matter further, but Plaintiff's only response was to file a motion for an Order to Show Cause on July 20, 2017.

It appears Plaintiff is seeking to force Let's Encrypt to revoke an SSL certificate and, should Let's Encrypt fail to do so within ten days (perhaps as early as ten days after the date the OSC issued), Plaintiff is also seeking a contempt finding and sanctions against Let's Encrypt. See, e.g., Plaintiff's Memorandum[4] at 20 (asking for an order "sanctioning . . . LE . . . for their contempt in an amount to be determined upon motion to the Court . . .)".

As discussed below, both the Default Judgment and the OSC are fatally flawed as applied to Let's Encrypt for four reasons. First, this Court lacks personal jurisdiction over Let's Encrypt, a California-based non-profit organization. Second, Let's Encrypt is not a party to this case and cannot be enjoined or sanctioned, as Plaintiff fails to meet its burden of proving Let's Encrypt is in active concert and participation with Defendants pursuant to Fed. R. Civ. P. 65. Third, the OSC violates Let's Encrypt's freedom of speech, as it seeks to prevent Let's Encrypt from making a true statement of fact – that on a particular date, specific domain was under the control of Defendants. Fourth, Let's Encrypt cannot be held in contempt as both the Default Judgment and the OSC are unenforceably

---

[3] *See Declaration of Benjamin A. Costa in Support of Non-Party Let's Encrypt's Memorandum of Law in Response to Order to Show Cause ("Costa Decl."), Exhibit C.*

[4] *July 21, 2017, Memorandum of Law in Support of Order to Show Cause (Docket #35) (the "Plaintiff's Memorandum").*

ambiguous.

As a result, Let's Encrypt asks the Court to deny Plaintiff's OSC and to award Let's Encrypt its attorney's fees and costs pursuant to Local Rule 83.6(d).

FACTUAL BACKGROUND

Let's Encrypt is a 501(c)(3) California non-profit corporation, with its principal place of business in San Francisco, California.[5] Let's Encrypt is a Certificate Authority ("CA") that, when requested, issues a type of signed Secure Socket Layer ("SSL") certificate known as a Domain-Validated ("DV") certificate. DV Certificates allow users to trust that a website with which they are communicating is not being impersonated or spoofed by an attacker.[6]

Overview of SSL, Certificates, and Secured Communications Channels

SSL is a means by which a user's communications with a website are secured from outsiders who may wish to observe, intercept, or alter those messages as they transit the internet. SSL operates by using a form of public-private key cryptography to securely exchange a single shared encryption key; the shared key is then used to encrypt the communications. Public Private Key Cryptography requires each party to have a pair of keys – one public and one private. Messages encrypted with the public key can only be decrypted with the matching private key; similarly, messages encrypted with the private key can only be decrypted with matching public key. Public keys are shared with anyone, while private keys are kept secret. This allows for others to ensure only the desired

[5] *See Aas Decl. at 4.*
[6] *See Cost Decl., Exhibit B.*

recipient can read a message – by using the recipient's public key to encrypt message, only the intended recipient (who has the matching private key) can decrypt the message.

SSL Certificates are one way in which a party can share their public key (and thus allow encrypted communications from another party). SSL Certificates include, at a minimum, the domain name of the website (e.g., "www.bob.com"), the public key of the certificate holder, the name of the issuer of the certificate, and the signature of the issuer. Anyone can create and sign their own certificates (a "self-issued" certificate), or they can create a certificate and send it to a CA as part of a request that the CA issue a signed certificate (known as a Certificate Signing Request or "CSR"). The SSL Certificate itself is not responsible for securing the communication channel – instead, the public-private key and the shared secret key are responsible. Attached as Exhibit D to the Costa Declaration is an example of a CA-issued DV Certificate.

There are different types of SSL Certificates, each of which carries different assurances from the CA about the certificate holder. The certificates issued by Let's Encrypt are known as "domain-validated" certificates ("DV Certificates"). In plain terms, a DV Certificate is a statement by Let's Encrypt that a specified domain was under the control of the certificate's holder at the time the holder requested the certificate from Let's Encrypt. DV Certificates allow users to validate that a domain they are connecting to is what it purports to be and not an imposter. DV Certificates do not contain any information about the identity of the holder of the certificate or make any assertions about the content available on the domain. Unexpected changes in control of a domain could indicate a security problem, such as a compromised website, a man-in-the-middle attack, or a spoofing attack.

Certificates are concerned with whether a website, as viewed by a site visitor, is in fact that website (as opposed to, for example, an imposter). Their presence or absence does not affect the content of a website, and customers can continue to buy infringing products whether or not a Certificate Authority revokes a website's certificates.

DV Certificates and Domain Transfers

DV Certificates are issued with respect to each domain name, not each owner. If a domain changes ownership, whether the certificate was revoked or not is irrelevant because (assuming the certificate is maintained) it will continue to function solely for the purposes explained above, including confirming to visitors that they are indeed at the website they requested, as opposed to an imposter site. Of the two domain names at issue in this Order to Show Cause – herbal-alchemist.com, and nfinx.com – herbal-alchemist.com is disabled, and nfinx.com redirects to another domain that does not use an SSL certificate. So, to the extent the instant order is directed to those domains it is effectively moot.

Let's Encrypt automatically issues domain-validated SSL certificates

Anyone can obtain – at no cost – a Let's Encrypt-issued domain-validated certificate. The process is automated and requires the certificate holder to submit their certificate signing request – including the holder's public key and other necessary information – to Let's Encrypt. Let's Encrypt then confirms that the certificate holder has control over the submitted domain name and, if so, signs the certificate. Let's Encrypt then issues the signed certificate by providing it to the requesting party. Over 47 million websites have used Let's Encrypt's service to receive DV Certificates, and Let's Encrypt is just one of many non-profit and for-profit providers of SSL certificates on the internet.

Let's Encrypt does not provide any encryption keys to requestors and the mere act of signing a certificate does not enable the certificate holder to protect their communications with SSL. Let's Encrypt does not charge a fee for its certificates, and provides them on an equal and automated basis to all who request them.[7] Let's Encrypt merely provides a general service to Defendants on the same terms as millions of other requestors. Beyond stating that on the date of the request, the certificate holder had control of the domain; Let's Encrypt has no relationship or affiliation with the Defendants whatsoever.

Let's Encrypt, by providing an SSL certificate, does not aid, abet, or enable trademark infringement. An SSL certificate can confirm a change in control of a domain, but is otherwise absolutely agnostic as to domain name, or content of any websites hosted on that domain.[8]

Let's Encrypt does not evaluate the content of a website before issuing an SSL security certificate. Let's Encrypt has no relationship with the certificate holder beyond issuing a signed certificate that validates the certificate holder's control of the domain at the time of the request.[9] Let's Encrypt has no control over how the certificate holder actually uses a domain, and Let's Encrypt does not control content placed or maintained on any website at issue in this litigation.[10]

Plaintiff's Misstatements about Let's Encrypt and DV Certificates

[7] *See Aas Decl. at 12.*
[8] *See Aas Decl. at 10.*
[9] *See Aas Decl. at 19.*
[10] *See Aas Decl. at 11.*

In its briefing, Plaintiff has on numerous occasions lumped Let's Encrypt in with the other non-parties it is seeking to enjoin, and has made a number of blanket statements about Let's Encrypt that are misleading or simply inaccurate. For example, in Plaintiff's Memorandum at 5, Plaintiff inaccurately states that the website's SSL certificate allows "Defendants to continue to securely operate . . . credit card purchases". Plaintiff has presented no evidence to support the assertion that Let's Encrypt certificates are in fact used in connection with payment processing. Typically, the SSL certificate of a third party payment processor – not the SSL certificate of the website – is used for secure e-commerce. Customers can also engage in credit card transactions with website lacking an SSL certificate, or websites using a self-signed certificate (though some browsers may issue a warning in these circumstances).[11] In other words, Plaintiff misleadingly implies that if the Court orders Let's Encrypt to revoke an SSL certificate, people will no longer be able to purchase goods from the site with a credit card. In point of fact, it's not clear that a Let's Encrypt certificate was even used in connection with payment on these sites, and Plaintiff has presented no more than conclusory statements in support of its assertion; at this time neither site is even accepting orders (because one is down and the other just redirects to another site.)[12] Regardless of the specific circumstances concerning Defendants' use of SSL, revoking the Let's Encrypt DV Certificate would not disrupt consumers' ability to buy products from the website.

---

[11] *Aas Decl. at 16.*

[12] *Plaintiff contacted Let's Encrypt after the OSC was entered seeking to have the DV Certificate for an additional site, cbd-now.com revoked. While the site uses a Let's Encrypt signed certificate for security, it not clear that it does so for the purpose of processing payments. Even if it did, removing the certificate would not stop the site from collecting payment, and would not stop the infringing activity.*

In Plaintiff's Memorandum at 12, Plaintiff inaccurately states that Let's Encrypt, among others, has "continued to advertise, promote and sell Defendants' infringing material on their websites."). Let's Encrypt has done no such thing. Let's Encrypt simply signs certificates in connection with its non-profit mission to promote a more secure World Wide Web. It has never advertised, promoted, or sold Defendant's material on its website. It has never mentioned any party to this litigation on its website, and has nothing whatsoever to do with this dispute, or the products at issue.

In Plaintiff's Memorandum at 13, Plaintiff inaccurately states that Let's Encrypt, among others, is ". . . profiting from allowing Defendants to advertise and/or sell the infringing products on their sites." Let's Encrypt has never advertised or sold, or allowed anyone else to advertise or sell any of Defendants' products on its site. Let's Encrypt is a 501(c)(3) nonprofit Certificate Authority, and does not profit from any of its activities; it issues DV Certificates for free to all parties who properly request them.

Let's Encrypt is not a party to this case nor does it operate in New York

Let's Encrypt is not a party to the *Herbalist & Alchemist, Inc. v. Alurent Products, Inc. and Will Clarent* action. Let's Encrypt is not a director, principal, officer, agent, representative, servant, employee, attorney, successor, or assign of the Defendants in the case. Other than issuing DV Certificates to members of the public, Let's Encrypt does not have any business relationship with the Defendants whatsoever. Let's Encrypt has never provided an SSL certificate to NameCheap, the entity the OSC commands Let's

Encrypt disable the SSL security certificate for.[13].

Let's Encrypt does not maintain any office or office space in the State of New York and does not have any employees or agents in New York. Let's Encrypt maintains no telephone number or mailing address in New York, and its website does not list any New York contact information. Let's Encrypt currently is not, nor has it ever been, authorized or licensed to do business in the State of New York. Let's Encrypt does not have an agent for service of process in New York. Let's Encrypt does not have, nor has it ever had, any member, parent, or subsidiary corporation located in the State of New York. Let's Encrypt does not own, nor has it ever owned, real or personal property located in the State of New York. Let's Encrypt does not incur or pay, nor has it ever incurred or paid, taxes in the State of New York. Let's Encrypt does not have a bank account in the State of New York. Let's Encrypt does not direct advertisement to or solicit business specifically in the State of New York. Let's Encrypt does not instruct any person or entity to advertise or solicit business in the State of New York on its behalf. Let's Encrypt operates a passive website that may be visible to users in any jurisdiction, and offers SSL certificate signing to parties who request them.[14]

LEGAL ARGUMENT

I. NON-PARTY LET'S ENCRYPT HAS NEVER ACTED IN CONCERT WITH DEFENDANTS TO VIOLATE AN ORDER OF THIS COURT AND CANNOT BE ENJOINED

---

[13] *See Aas Decl. at 21.*

[14] *See Aas Decl. at 22-26.*

Rule 65 of the Federal Rules of Civil Procedure codifies the "well-established principle that, in exercising its equitable powers, a court 'cannot lawfully enjoin the world at large.'"[15] Non-parties that are not agents can only be bound if they are in "active concert or participation" with the Defendants.[16] The "active concert or participation" standard is narrow only ensures that "defendants may not nullify a decree by carrying out prohibited acts through aiders and abettors[.]"[17] The relationship between the party and the nonparty must be "that of associate or confederate."[18]

Let's Encrypt has only the most minimal of relationships with Defendants – it automatically issued signed DV Certificates to domains Plaintiff alleges are owned by Defendants. As discussed below, this is insufficient to meet the strict standard required to bind a non-party to an injunction and Plaintiff's motion should be rejected.

A. LET'S ENCRYPT DOES NOT AID AND ABET ANY INFRINGING ACTIVITIES BY DEFENDANTS

Let's Encrypt is not a party to this case. Nor is Let's Encrypt an agent of Defendants.[19] Let's Encrypt has not participated in any of the allegedly-wrongful acts committed by Defendants. Let's Encrypt's only relation to this case is through its role as a Certificate Authority. Any certificates issued to Defendants were automatically issued in

---

[15] *New York v. Operation Rescue Nat'l, 80 F.3d 64, 70 (2d Cir. 1996) (quoting Alemite Mfg. Corp. v. Staff, 42 F.2d 832, 832 (2d Cir. 1930) (Hand, J.)).*

[16] *Fed. R. Civ. P. 65(d)(2); see also United States v. Kirschenbaum, 156 F.3d 784, 794 (7th Cir. 1998).*

[17] *Regal Knitwear Co. v. NLRB, 324 U.S. 9, 14 (1945).*

[18] *Chase Nat'l Bank v. City of Norwalk, Ohio, 291 U.S. 431, 436-37 (1934); see also Microsystems Software, Inc. v. Scandinavia Online AB, 226 F.3d 35, 43 (1st Cir. 2000) ("[A]ctive concert" requires a "close alliance with the enjoined defendant").*

[19] *See Aas Decl. at 19.*

the same manner as the other 47 million certificates Let's Encrypt has issued, and in the same manner as the hundreds of other CAs have issued such certificates.

Let's Encrypt issues DV Certificates to millions of requestors automatically and as arms-length transactions. Each certificate is, in effect, merely a statement by Let's Encrypt that, on the date requested, the requestor had control of the specific domain name. In no way does Let's Encrypt aid, abet, act in concert or participation with, or otherwise intentionally or knowingly assist the Defendants in violating an injunction. Just as a telephone company cannot be required to withdraw telephone service from a customer just because the customer might discuss an infringing product on the telephone, Let's Encrypt cannot be required to revoke DV Certificates merely because a website might be put to bad use. Rule 65 requires a much more specific showing before an injunction may be deemed to apply to a non-party. Non-parties can only be bound if they are shown to be working in "active concert or participation" with Defendants.[20] This is a narrow standard, that requires the nonparty to be acting as an "associate or confederate" to "aid and abet" the Defendant in violating an injunction.[21] If, instead, the non-party acts "independently of the enjoined defendant [then the non-party] will not be bound by the injunction."[22]

Non-parties cannot be enjoined for engaging in arms-length transactions with Defendants.[23] For example, in *Blockowicz v. Williams*, 630 F.3d 563 (7th Cir. 2010), the

---

[20] *Fed.R.Civ.P. 65(d)(2)(C).*

[21] *Chase Nat'l Bank, 291 U.S. at 436-37; Microsystems Software, Inc., 226 F.3d at 43.*

[22] *Microsystems Software, 226 F.3d at 43.*

[23] *ONE11 Imps. Inc. v. NuOp LLC, No. 16-CV-7197 (JPO), 2016 U.S. Dist. LEXIS 175160 at *5 (S.D.N.Y. Dec. 19, 2016). (holding nonparty retailers and distributors could not be enjoined from selling infringing materials).*

Seventh Circuit held that the operators of a nonparty website could not be bound by an injunction against users of its service who posted defamatory comments about the Plaintiff, even though the nonparty had a contracts with the users and continued to host the users' material online. *Id*. at 567-68. The court noted that even if a non-party "is technologically capable of removing the postings [this] does not render its failure to do so aiding and abetting." *Id*. at 568. Courts in New York have reached similar conclusions.[24]

Let's Encrypt has entered into only the most minimal of arms-length transactions – it issued a DV Certificate, in an automated manner, that simply states that the certificate holder controlled a domain on a given date. This fact is not subject to copyright or trademark protection and cannot aid or abet infringement. Like the non-party website in *Blockowicz* and the non-party retailers in *Paramount Pictures*, Let's Encrypt has not acted in active concert or participation with the Defendants and thus cannot be enjoined. Although Let's Encrypt believes that *Arista Records* v. *Tkach*, 122 F.Supp.3d 32 (S.D.N.Y. 2015) was wrongly decided, the facts of Let's Encrypt's DV Certificate issuance are distinguishable. Let's Encrypt's service is automated, passive, does not carry or transmit any website content, does not connect users to infringing content or products, and is not necessary for (and indeed may have never been used in connection with) purchasing products. In addition, the domains in question are no longer operating to serve content.

---

[24] *See, e.g., Hammer v. Trendl, No. CV02- 2462ADS, 2002 WL 32059751, at *4 (E.D.N.Y. 2002) (refusing to enjoin non-party websites that hosted defamatory reviews by the Defendant); Paramount Pictures Corp. v. Carol Publ'g Grp., 25 F. Supp. 2d 372, 374-75 (S.D.N.Y. 1998) (nonparty retailers and distributors could not be enjoined from selling an infringing book.).*

The sum total of Plaintiff's allegations concerning Let's Encrypt is that Let's Encrypt is purportedly "aiding and abetting Defendants' infringing activities by providing Defendants with a secure means by which to sell its products online with credit card." Yet Plaintiff has presented no evidence that any Let's Encrypt DV Certificate issued to Defendants has been used for processing credit card payments. The common practice is the opposite – most websites use a third-party payment processor, which only relies upon the payment processor's certificate, not the website's certificate, to secure the payment.[25] One of Defendants' websites seems to have operated in this fashion – herbal-alchemist.com's privacy policy stated that customer information "is transmitted securely to our third part[y] processing provider in compliance with Payment Card Industry standards."[26]

Furthermore, even if a Let's Encrypt issued a DV Certificate were used to verify that a domain accepting payment was not an imposter, Let's Encrypt does not offer or provide payment processing services, and can neither enable nor prevent customers from buying products over the internet. Let's Encrypt certificates are not specific to payment processing domains and are not specifically provided for the purpose of operating a payment processing system. Aas Decl. at 13.

All the DV Certificate does is enable a website to prove that it is what it purports

---

[25] *Aas Decl. at 14.*

[26] *See Herbal Alchemist Privacy Policy (Wayback Machine capture from Nov. 10, 2016; available at https://web.archive.org/web/20161110152300/https://herbal-alchemist.com/privacy-policy); Aas Decl. at 15; see also Costa Decl., Exhibit A.*

to be to its visitors, and to protect their communications with it from interception, redirection, and manipulation. Let's Encrypt's certificate services do not facilitate intellectual property infringement of any kind. All that Let's Encrypt offers is a way to verify that a domain is not an imposter – and this is insufficient to either constitute infringement or to meet strict requirements to enjoin a non-party.[27]

B. PLAINTIFF'S REMEDY IS AGAINST DEFENDANTS, NOT THROUGH ENJOINING DOZENS OF NON-PARTIES

Plaintiff seeks the wrong remedy. Through its OSC, Plaintiff seeks to rewrite Fed. R. Civ. P. 65 to permit injunctions against any non-party, to bar any form of service to an enjoined party, no matter how remote the relationship between non-party and defendant or between service and defendant misconduct. This unprecedented expansion would violate due process rights by allowing injunctions to issue without the opportunity for the non-party to be heard first. If Plaintiff's request is granted, other parties may seek the same remedy, using allegations of trademark or copyright infringement to obtain orders against the world. New York courts have regularly rejected such efforts, declining to enjoin non-parties who are not actively assisting a defendant even when such an injunction arguably would have benefitted the plaintiff.[28]

---

[27] *See, e.g., Perfect 10 v. Visa Int'l Service Ass'n, 494 F.3d 788 (9th Cir. 2007) (even though Visa knew about infringement, and processed payments for allegedly infringing goods, merely processing payments did not materially contribute to infringement; to hold otherwise would extend liability to service providers related to any transaction where infringing material is bought or sold).*

[28] *See, e.g., CommScope, Inc. of North Carolina v. Commscope (U.S.A.) Intern. Group Co., Ltd., 809 F. Supp. 2d 33, 42 (N.D.N.Y. 2011) (declining to direct non-party Secretary of State to dissolve trademark infringing defendant's corporate name), see also Pitbull Productions, Inc. v. Universal Netmedia, Inc., No. 07 Civ. 1784(RMG)(GWG), 2007 WL 3287368, at *7 (S.D.N.Y. 2007) (declining to grant injunction ordering non-party GoDaddy to take down a website infringing plaintiff's trademark).*

This Court need not risk the dangers of adopting Plaintiffs' near-limitless expansion of "active concert and participation." Instead, there is a simpler, cleaner, and easier solution – once plaintiffs, through the process of litigation against their chosen defendants, are granted control of defendants' domains pursuant to court order, plaintiffs can disable any websites associated with the domain names they receive. Furthermore, Let's Encrypt's DV Certificates are only valid for 90 days – after that period, they expire and a new CSR must be submitted from the domain itself. Thus, if the domain is disabled or if control has transferred to Plaintiff, no new certificates will issue.

Plaintiff has already secured an order requiring that certain domains be transferred in this case, and requiring Defendants to cease using the domains for the purportedly infringing conduct. This order has already worked – both domains are inactive. Though one domain redirects elsewhere, the domain it redirects to has no SSL certificate, and if there is infringing content on it Plaintiff is free to request that the court order appropriate relief against the owners of it. Although Let's Encrypt is simply not in a position to be able to meaningfully assist with Plaintiff's problem, Plaintiff is not without recourse – recourse that in this case seems to have already worked.

Transfer of the domain is the appropriate remedy when a domain name itself infringes a trademark – revocation of the DV Certificate is not, nor would revocation address the infringement at issue. Websites are not required to enable (or force) SSL communications (or acquire or create any type of SSL certificate in the first instance) and withdrawal of the DV Certificate does not affect ownership of the domain name, change the allegedly infringing domain name, alter the content and products available at the domain, or affect any other feature of the domain. See Aas Decl. at 18. All revocation

does is put innocent users at risk.

Plaintiff could have chosen surgically to seek enforcement only against those non-parties with the power to directly address the infringing conduct. Instead, Plaintiff has chosen indiscriminately to go after over a dozen non-parties, seemingly because these non-parties might have some relation to how a potential customer might try to contact the Defendants or Defendants' website.

Rather than holding dozens of non-parties in contempt of an ambiguous order, Let's Encrypt asks the Court to require Plaintiff to obtain domain transfer directly, as is appropriate in cases of this type. Once Plaintiff has taken control of the domain name, the SSL certificate (should they choose to maintain it) will function for the purpose it always has: securing communications between the website (regardless of its owner) and visitors to the website (regardless of the purpose of their visit).

II. LET'S ENCRYPT SHOULD NOT BE HELD IN CONTEMPT OF THE DEFAULT JUDGMENT BECAUSE IT IS AMBIGUOUS

A court may hold a party in contempt only if (1) the order the party failed to comply with is clear and unambiguous, (2) the proof of noncompliance is clear and convincing, and (3) the party has not diligently attempted to comply in a reasonable manner.[29] An injunction is clear and unambiguous only if it leaves "no doubt in the minds of those to whom it was addressed . . . precisely what acts are forbidden."[30] Ambiguity is determined based only on the language of the injunction itself – a party "must be able to

---

[29] *CBS Broad. Inc. v. FilmOn.com, Inc. (2d Cir. 2016) 814 F.3d 91, 98 (quoting Paramedics Electromedicina Comercial, Ltda. v. GE Med Sys. Info. Techs. Inc., 369 F.3d 645, 655 (2d Cir. 2004)).*

[30] *Id. at 98 (quoting Druwall Tapers & Pointers v. Local 530, 889 F.2d 389, 395 (2d Cir. 1989)).*

ascertain from the four corners of the order precisely which acts are forbidden."[31] It is unclear whether Plaintiff seeks, by way of the Order to Show Cause, to sanction Let's Encrypt for some undefined contempt of the Default Judgment or whether, instead, it seeks to require Let's Encrypt to comply with any issued form of the Order to Show Cause within 10 days upon threat of contempt and sanctions for violation of the OSC.

As discussed below, Let's Encrypt cannot be sanctioned or held in contempt of these ambiguous orders and Plaintiff's motion to do so should be denied.

A. LET'S ENCRYPT SHOULD NOT BE HELD IN CONTEMPT OF THE DEFAULT JUDGMENT BECAUSE IT IS AMBIGUOUS

If Plaintiff is seeking to sanction Let's Encrypt for a failure to comply with the Default Judgment, such a sanction is not warranted. Even assuming, for the purposes of argument, that the Default Judgment could bind non-parties, a contempt finding is not appropriate because a non-party reading the Default Judgment would be unable to determine whether or not it forbids the issuance of SSL certificates. If a non-party cannot determine, from the face of an order, the specific acts that are forbidden, the order is ambiguous and unenforceable.

The Default Judgment purports to enjoin the Defendants, the agents of the Defendants, and "all others in active concert or participation with Defendants" from infringing uses of the Plaintiff's trademark, from false statements about Plaintiff's products, from false advertising, and the like.[32]

---

[31] *Drapwall Tapers & Pointers v. Local 530, 889 F.2d 389, 395 (2d Cir. 1989).*

[32] *Default Judgment at 3.*

None of the categories mention issuing DV Certificates (or issuing any other form of SSL certificate). Nor do any of the categories purport to bar factual statements about who controls a given domain name at a given time, which is all a DV SSL certificate does.[33] Finally, the Default Judgment does not name Let's Encrypt or any other non-party service provider.

The party seeking a contempt finding bears the heavy burden of establishing the claim by clear and convincing evidence.[34] Specifically, the movant must demonstrate by clear and convincing evidence that (i) a valid court order was in effect, (ii) that order clearly and unambiguously required certain conduct by the respondent, and (iii) the respondent failed to comply with the court's order.[35]

Since Let's Encrypt is not acting in active concert or participation with the Defendants in this case, has done nothing to facilitate the Defendants' infringement, is not aware of being bound by any current clear and unambiguous order of the Court concerning the issuance or revocation of certificates, and is not otherwise subject to this court's jurisdiction, a finding of contempt or sanction would be inappropriate at this time.

---

[33] *For this reason, Let's Encrypt also believes that an order enjoining it from issuing a DV SSL certificate would also violate the First Amendment. See, e.g., Met. Opera Ass'n v. Local 100, Hotel Employees and Rest. Emp. Intern. Union, 239 F.3d 172 (2d Cir. 2001) (reversing the grant of an injunction that restricted freedom of speech of a party).*

[34] *Stringfellow v. Haines, 309 F.2d 910, 912 (2d Cir. 1962).*

[35] *King. v. Allied Vision, Ltd., 65 F.3d I051, 1058 (2d Cir. 1995); see also Levin v. Tiber Holding Corp., 277 F.3d 243, 251 (2d Cir. 2002) ("It must be proven that [the alleged contemnor] 'had knowledge of and disobeyed a clear, explicit and lawful order of the court and that the offending conduct prejudiced the right of the [other] party.'") (internal citation omitted).*

B. LET'S ENCRYPT SHOULD NOT BE HELD IN CONTEMPT BECAUSE THE ORDER TO SHOW CAUSE IS AMBIGUOUS

The Order to Show Cause is also ambiguous on a number of points. For example, it is not clear whether it purports to require compliance with 10 days of the Order to Show Cause, within 10 days after service of the Order to Show Cause, or within 10 days of an order the Court might issue following the hearing on the Order to Show Cause.

In addition, the Order directs Let's Encrypt "to withdraw the SSL Certificate for Namecheap." Let's Encrypt is not aware of any certificates that it has issued to Namecheap. Rather, it appears that Namecheap's certificate was issued by Comodo Group, a CA unaffiliated with Let's Encrypt.[36] Because it did not issue Namecheap's SSL certificate, Let's Encrypt cannot withdraw Namecheap's SSL certificate. Assuming the Order was incorrect and instead referred to one of the other domains referenced therein (herbal-alchemist.com and/or nfinx.com), the Order is ambiguous as to which (if any) it is referencing; neither domain has content on it anymore and therefore such an order would be moot; and, as discussed above, Rule 65 is not broad enough to cover a provider of a DV SSL certificate in this context.

III. LET'S ENCRYPT CANNOT BE ENJOINED BY THE DEFAULT JUDGMENT OR REQUESTED ORDER AND SHOULD NOT BE HELD IN CONTEMPT BECAUSE THE COURT LACKS PERSONAL JURISDICTION OVER IT.

Established law holds that "one is not bound by a judgment *in personam* resulting from litigation in which he is not designated as a party or to which he has not been made a

---

[36] *See Aas Decl. at 21.*

party by service of process."[37] In addition, "a court has no power to adjudicate a personal claim or obligation unless it has jurisdiction over the person of the defendant." *Id.* This requires a finding that personal jurisdiction exists and that exercising personal jurisdiction would not violate Let's Encrypt's due process rights.[38]

In this case, neither New York's general jurisdiction nor long-arm statutes provide a basis for this Court to exercise personal jurisdiction over Let's Encrypt. Additionally, and while the Court need not reach this issue, Let's Encrypt also lacks the minimum contacts with New York necessary for this Court to exercise personal jurisdiction over it consistent with the requirements of the Due Process Clause. As a result, Plaintiff's motion should be denied.

A. LET'S ENCRYPT IS NOT "DOING BUSINESS" IN NEW YORK UNDER C.P.L.R. 301.

Pursuant to C.P.L.R. §301, a defendant is subject to personal jurisdiction in New York if it is "doing business" in New York. This standard requires that a party be "engaged in such a continuous and systematic course of 'doing business' in New York as to warrant a finding of its 'presence' in the state."[39] "[A] corporation is 'doing business' and is therefore 'present' in New York and subject to personal jurisdiction with respect to any cause of action, related or unrelated to the New York contacts, if it does business in New York, not occasionally or casually, but with a fair measure of

---

[37] *Zenith Radio. Corp. v. Hazeltine Research, Inc., 395 U.S. 100, 110 (1969).*

[38] *Digisound-Wie, Inc. v. Bestar Technologies, Inc., No. 07-6535, 2008 WL 2095605 (N.D.Ill. May 16, 2008); see also Cutco Indus., Inc. v. Naughton, 806 F.2d 361, 365 (2d Cir. 1986) (looking to New York law to determine whether the E.D.N.Y. could exercise in personam jurisdiction over a nonresident defendant); International Shoe Co. Washington, 326 U.S. 310, 316 (1945).*

[39] *Jazini v. Nissan Motor Co., Ltd., 148 F.3d 181, 184 (2d Cir. 1998) (internal citations omitted).*

permanence and continuity."[40]

In determining whether a defendant is subject to general jurisdiction, New York courts look to a number of factors, including: the existence of an office in New York; the solicitation of business in the state; the presence of bank accounts and other property in the state; and the presence of employees of the foreign defendant in the state.[41] Even where one or more factors are present, courts may conclude that the contacts with the state are insufficient to justify the exercise of general jurisdiction.[42]

Let's Encrypt is physically located outside of New York, is not incorporated in the state, has no employees or office in the state, has no continuous business presence in the state, is not licensed to do business in the state, and has no agent designated to receive service of process in the state. See Aas Decl. at 22-26.

While Let's Encrypt DV Certificates are globally available via the internet, including in New York, "the fact that a foreign corporation has a website accessible in New York is insufficient to confer jurisdiction under C.P.L.R. § 301."[43] Let's Encrypt certificates are analogous to such a website: they are generally available to all internet users, who may request and receive them without the direct intervention of the employees of Let's Encrypt. Accordingly, Let's Encrypt is not "doing business" in New York such

---

[40] *Wiwa v. Royal Dutch Petroleum Co., 226 F.3d 88, 95 (2d Cir. 2000).*

[41] *Hoffritz for Cutlery, Inc. v. Amajac, Ltd, 763 F.2d 55, 58 (2d Cir. 2000).*

[42] *See, e.g., Xiu Feng Liv. Hock, 371 Fed. Appx. 171, 174 (2d Cir. 2010) ("Solicitation of business alone will not justify a finding or corporate presence in New York with respect to a foreign manufacturer or purveyor of services."); Canadian Group Underwriters Ins. Co. v. M/V Arctic Trader, No. 96-9242, 1998 WL 730334, *3 (S.D.N.Y. Oct. 19, 1998) (existence of bank account used to wire out funds, agreement to arbitrate disputes in New York and presence of registered agent in New York not sufficient to show that defendant was doing business in New York).*

[43] *Spencer Trask Ventures v. Archos SA., No. 01-1169, 2002 WL 417192, at *6 (S.D.N.Y. March 18, 2002).*

that general jurisdiction is appropriate under C.P.L.R. § 301.

B. LET'S ENCRYPT LACKS SUFFICIENT CONTACTS WITH NEW YORK TO JUSTIFY THE EXERCISE OF SPECIFIC JURISDICTION UNDER C.P.L.R. § 302(A)(L).

Further, Let's Encrypt is not subject to specific jurisdiction under New York's long-arm statute, N.Y. C.P.L.R. 302 (a). To establish specific jurisdiction under this statute, there must be "an articulable nexus, or a substantial relationship" between the claim asserted and the actions that occurred in New York."[44] Let's Encrypt is outside of the reach of the long-arm statute because it is physically located outside of New York, is not incorporated in the state, has no employees or offices in the state, has no continuous business presence in the state, is not licensed to do business in the state, has never owned real or personal property that is located in New York, does not direct advertisement to or solicit business specifically in New York, and has no agent designated to receive service of process in the state. See Aas Decl. at 22-26. Again, the only contact that Let's Encrypt has with New York is the fact that its generally-accessible SSL security certificate services are accessible from that state – as they are in every other jurisdiction that has access to the internet. The availability of Let's Encrypt certificates does not constitute "transacting business" for the purpose of Section 302 unless coupled with some additional connection to New York.[45]

---

[44] *Best Van Lines, Inc. v. Walker, 490 F.3d 239, 246 (2d Cir. 2007).*

[45] *See, e.g. ISi Brands. Inc. v. KCC Intern. Inc. 458 F.Supp.2d 81, 87-88 (E.D.N.Y. 2006) (noting that "[e]ven the existence of an interactive 'patently commercial' website that can be accessed by New York residents is not sufficient to justify the exercise of personal jurisdiction unless some degree of commercial activity occurred in New York.").*

C. THE EXERCISE OF PERSONAL JURISDICTION OVER LET'S ENCRYPT WOULD VIOLATE DUE PROCESS.

Because Let's Encrypt does not have even minimum contacts with the State of New York, the Court's exercise of personal jurisdiction over Let's Encrypt would also fail to comport with constitutional due process requirements.[46]

In order to meet the constitutional due process standard, a district court must find that the non-resident defendant has purposefully established "minimum contacts" in New York and that the quality and nature of defendant's contacts are "such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice."[47]

New York State's long-arm statute does not extend jurisdiction to the furthest extent permissible under the U.S. Constitution.[48] Instead, to determine whether the requisite contacts exist, courts consider: "(1) whether the defendant purposefully availed himself of the benefits of the forum state; (2) whether the defendant's conduct and connection with the forum state are such that he should reasonably anticipate being hailed into court there; and (3) whether the defendant carries on a continuous and systematic part of its general business within the forum state."[49]

Here, none of these factors can be met consistent with the requirements of due

---

[46] *See Berwick v. New World Network Intern., Ltd., No. 06-2641, 2007 WL949767, at *9 (S.D.N.Y. March 28, 2007); Sunward Electronics, Inc. v. McDonald, 362 F.3d 17, 24 (2d Cir. 2004).*

[47] *International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945); City of New York v. CycoNet, 383 F.Supp.2d 526, 541 (S.D.N.Y.2005) ("In determining whether minimum contacts exist, the court considers 'the relationship among the defendant, the forum, and the litigation.") (internal citation omitted).*

[48] *Local 875 J.B.T Pension Fund v. Pollack, 992 F.Supp. 545 (E.D.N.Y. 1998).*

[49] *Baron Philippe de Rothschild, SA. v. Paramount Distillers, Inc., 923 F.Supp. 433, 437 (S.D.N.Y. 1996); Burger King Corp. v. Rudzewicz, 471 U.S. 462, 473-4 (1985).*

process. Let's Encrypt does not specifically target the State of New York as a place of business, nor does it have any continuous and systematic contact with the state. See Aas Decl. at 22-26. Let's Encrypt does not participate in any purposeful activity such that it could foresee being hailed into court in the State of New York. Indeed, the only contact that Let's Encrypt has with New York is that its certificates can be accessed from the state. To find that this activity subjects Let's Encrypt to personal jurisdiction in New York would render Let's Encrypt amenable to jurisdiction in every state. Such a finding would violate the guarantee of due process. Therefore, the Southern District of New York's exercise of jurisdiction over Let's Encrypt does not survive constitutional scrutiny.

IV. THE COURT SOULD AWARD LET'S ENCRYPT ITS COSTS AND ATTORNEYS' FEES IN CONNECTION WITH THIS RESPONSE

SDNY Local Rule 83.6(d) provides that if an alleged contemnor is found not guilty of contempt, "said person shall be discharged from the proceedings and, in the discretion of the Court, may have judgment against the complainant for costs and disbursements and a reasonable counsel fee." Plaintiff has made a number of inaccurate and misleading statements in its brief, ranging from its implication that Let's Encrypt is somehow necessary to Defendants' ability to accept credit card payments, to outright misstatements that Let's Encrypt hosts infringing content and carries advertising for Defendants. Plaintiff's carelessness has also extended to the "shotgun" manner in which it elected to prosecute this matter against non-party, neutral service providers who have nothing to do with the subject matter of this litigation.

The Court should award Let's Encrypt its costs and reasonable attorney's fees,

because using a default judgment to force every conceivable third-party service provider to show up in a faraway court to explain why they are not in contempt is unreasonable, vexatious, and unduly burdensome; because Plaintiff apparently exercised little or no forethought about whether such proceedings were justified or whether the third party service providers were subject to the jurisdiction of this court; and because Plaintiff's argument that Let's Encrypt was in "active concert and participation" with the Defendants in this case is objectively unreasonable and baseless.

CONCLUSION

For these reasons, Let's Encrypt respectfully requests the Court find that Let's Encrypt is not in contempt, issue an appropriate order discharging Let's Encrypt from any further involvement in these proceedings, grant Let's Encrypt its attorneys' fees and costs, and grant such other relief to Let's Encrypt as the Court deems appropriate under these circumstances.

Dated: August 7, 2017
New York, NY

Stramiello Law Firm

/s/ Warren A. Stramiello
(warren@law.stramiello.net)
5 Masefield Lane
Hartsdale, NY 10530
Tel: (678) 619-1337
Fax: (415) 423-3571

Ridder, Costa & Johnstone LLP
Chris K. Ridder
CA Bar No. 218691 (pro hac vice pending)
(chris@rcjlawgroup.com)
12 Geary Street, Suite 701
San Francisco, CA 94108
Tel: (415) 391-3311
Fax: (415) 358-4975

Attorneys for Non-Party Internet Security Research Group, dba Let's Encrypt